DEVELOPMENT OF CRYPTO-BIOMETRIC SYSTEM USING FINGERPRINT AND RSA MODEL FOR SECURE COMMUNICATION

By

NOEL MOSES DOGONYARO * WAZIRI ONOMZA VICTOR ** SHEIDU KAKA JUMAI ***

*-*** Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria.

Date Received: 22-04-2020 Date Revised: 14-05-2020 Date Accepted: 17-06-2020

ABSTRACT

A communication system is a system model that describes a communication exchange between two stations, transmitter and receiver. The application of cryptography is treated as the most effective solution to ensure the secure transmission of data. Cryptographic drawbacks cause such systems to cryptanalysis by malicious individuals, resulting in most data breaches. As an alternative, this system proposes a framework that provides solution to communication system by integrating biometrics with cryptography. The system developed makes use of the combination of public key RSA system with fingerprint, which is the most popularly used biometric. This research work ensures the security of messages communicated between the two users and the maintenance of a secure authentication mechanism. The developed system is based on privacy-preserving architecture. It could be used as an access control system as well as an internal communication mechanism for many organizations.

Keywords: Biometric, Communication, Decryption, Encryption, Security.

INTRODUCTION

Information security has always been the focus of security experts. When communication is a daily necessity, the protection of static data or data in transit always causes problems because it always surrounds the malicious individual who seeks to disrupt the confidentiality, integrity and availability of information. (Chebotareva et al., 2018). Communication uses transmission channels to pass information from one device to another. According to Aanjanadevi et al. (2019), transmission channels are often insecure because of poor security mechanism. These security mechanisms have created many security problems, such as denial of audited communication events (repudiation) by persons, and other kinds of felonious actions like malicious hacking into legitimate user's accounts, cyber bullying, sending spoofed and phishing messages, resulting in either data losses or sensitive information leakage. When this occur, defaming of individual integrity of the involved persons raises curiosity on the need to adopt powerful and more reliable methods to verify the identity of the persons.

The application of crypto-biometric principle for secure communication plays a vital role in ensuring that the security of sensitive data is maintained while in transit. Biometrics system as defined by Adamovic et al. (2016) is the automated recognition of individuals based on their behavioral and biological characteristics. This technology is mainly adopted for the authentication and identification of the involved personnel's and can be Uni-modal (i.e., rely on the evidence of a single source of information for authentication, for example, single fingerprint or face) or Multi-biometric (ie., they rely on the evidence including multiple sources of information for establishing identity). Since, the advent of the internet and the growing rise in communication consists of different problems, information security has been the focus of security experts globally (Afriyie & Arkorful, 2019). Once relied upon traditional methods of encryption are insecure as they are subjected to cryptanalysis (the act of deciphering coded messages without being told the key) by individuals who disrupt the fundamentals of Information Security, including Confidentiality, Integrity,

Authentication, Availability and Non-Repudiation of data either static or on transit. Incorporating the most commonly used form of biometric solution which is the fingerprint with the widely used asymmetric encryption solution, the Rivest-Shamir-Adleman (RSA), addressing and proposing a solution to the afore-mentioned issues using a Crypto-biometric System is assumed to be the proffer solution in a communication system.

1. Review of Related Literature

To ensure secure transmission of data over a communication channel, cryptographic algorithms such as RSA are often regarded as the most effective solution. The integration of cryptographic algorithms and traditional biometric systems has gained more popularity in the field of information security. In an attempt to strengthen the security among communication parties, Barman et al. (2015) proposed an approach for generating cryptographic keys from cancellable fingerprint template of both communication parties in order to avoid key storage without compromising the strength in security. The authors aimed at solving the problem of key management using RSA and fingerprint data. Similar work was carried out by Jin et al. (2016) using an Elliptic Curve Cryptography-free binding scheme with cancelable transforms for minutiae-based fingerprint biometrics instead of fuzzy commitments. The main idea for key binding approach is to secure the biometric template by binding it with the cryptographic key. However, the limitation of this approach is that fuzzy commitments suffer from security (key size) performance. With this limitation, Adamovic et al. (2016) considers a method based on information-theoretic analysis of iris biometric that aims at extracting the homogeneous regions of high entropy. The authors believed that successful extraction of these regions facilitates the development of an effective system for generating cryptographic keys of lengths up to 400 bits per iris. Similarly, a Tri-Layered approach was used by Osho et al. (2019) to develop a system known as "Absolute secure". The authors developed a multi-layer data security that leverages on biometric, cryptography, and steganography for securing data. However, the system developed requires high memory consumption and takes a lot of hardware resources during execution. Dwivedi et al. (2019) developed a framework for secure communication among users on a network using crypto-biometric technique. In this approach, the Diffie Hellman algorithm was used to generate public keys from private keys of sender and receiver. However, the major issue with this framework is key revocation and key distribution. Saad (2019) performs a systematic review on the use of biometric authentication system security in Automated Teller Machine (ATM) for the past 15 years of inception while Shenoy and Shaikh (2019) focuses on using cryptography and steganography as an alternative secure method for data transfer in a network.

2. Overview of Cryptobiometrics

Since 1998, a new innovative multidisciplinary research field denoted as crypto-biometrics has emerged. According to Dwivedi et al. (2019), biometrics is integrated with cryptography which is the science of keeping transmitted data secure, but requires better verification mechanisms that now adopt a security mechanism known as crypto-biometric system in order to alleviate the limitations of generic biometric systems (Barman et al., 2015). Crypto-biometric systems help improve the privacy issues of biometric systems, by obtaining cryptographic keys and the protection of biometric data from biometrically generated cryptographic keys. Crypto-biometric systems have the following classifications namely key release, key generation and key regeneration.

In key release approach, a randomly created and stored cryptographic key is protected from unauthorized access with user' biometric data and release them only after successful biometric verification (Aggarwal & Maurer, 2016). In key generation, a binary string is generated from the users biometric, resulting in a template free biometric system where the need for template storage is eradicated as there is only a need to store the already generated verifying binary string.

In key regeneration, cryptographic techniques are used to bind a key that has been generated at random with the

biometric data and the resulting key from the binding process is used for verification.

3. Analysis of Existing Systems

Presently, there are many commercial and open- source communication systems on the internet but only a few have used crypto-biometric system security and vice versa. The work of Osho et al., (2014) is considered as baseline research. In this work, the system developed provides a certain level of security due to the integration of biometric, cryptography and steganography, although the system used a mechanism that is vulnerable to cryptanalysis and steganalysis. For the cryptography integration, the system proposed the use of Advanced Encryption Standard (AES-128), which uses a simple algebraic structure with every block being encrypted in the same way as such it can be cryptanalyzed. While trying to incorporate steganography, Least Significant Bits (LSB) technique is the simplest to understand and implement, resulting in the use of stenographic image proving to be unsafe. It is the reason for this research to be proposed a more secure crypto-biometric system that combines biometric (fingerprint) and cryptography (RSA) and compared with the existing systems.

4. System Analysis and Design

The first design process was the fingerprint image pre-processing, which involved image enhancement (making it clearer), image binarization (i.e., choosing optimal threshold for each image area to perform 256 gray levels conversion to a black and white image), and image thinning (i.e., reducing the image thickness as possible). This was followed by developing a fingerprint enrolment model.

During the enrolment process, one or more fingers are scanned or captured by each person to retrieve the Fingerprint Image Data (FID) which is then used to enroll the person. This image is then processed using a user specific algorithm to obtain the abstinent minutiae features. These features are encrypted and hashed for security reason, which are then used to create a referenced biometric template with a referenced hash for the user in a secure database that will be matched for recognition. Figure 1 is the block diagram of the secure fingerprint enrolment process.

The stages involved in the fingerprint recognition process are presented in Figure 2.

5. Architechtural Design

Figure 3 is the crypto-biometric architectural design. From the designed system, to perform revocable transformation, it means that for every bit string obtained, a binary string is produced by the permutation of a random key. A resulting private key of 256-bit is generated from the binary hashing of the bit string using SHA256, which is used as an input to the RSA algorithm for generating the sender and receiver public keys using two predefined parameters. These public keys are then shared between sender and receiver. The RSA algorithm uses the senders own private key and the recipient public key to generate a symmetric key at the end of both users. This key is termed as intermediate key, which is further

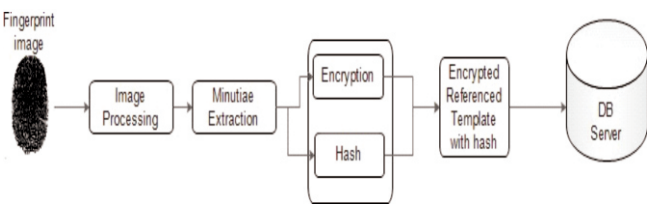

Figure 1. Fingerprint Enrollment Process

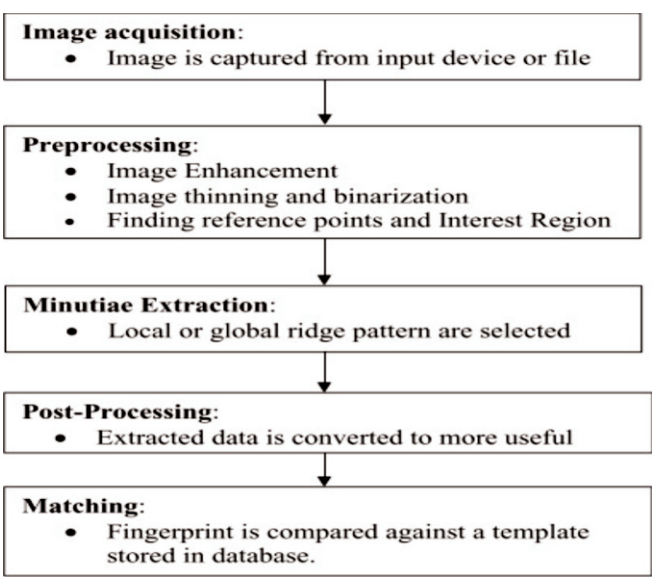

Figure 2. Fingerprint Recognition Process

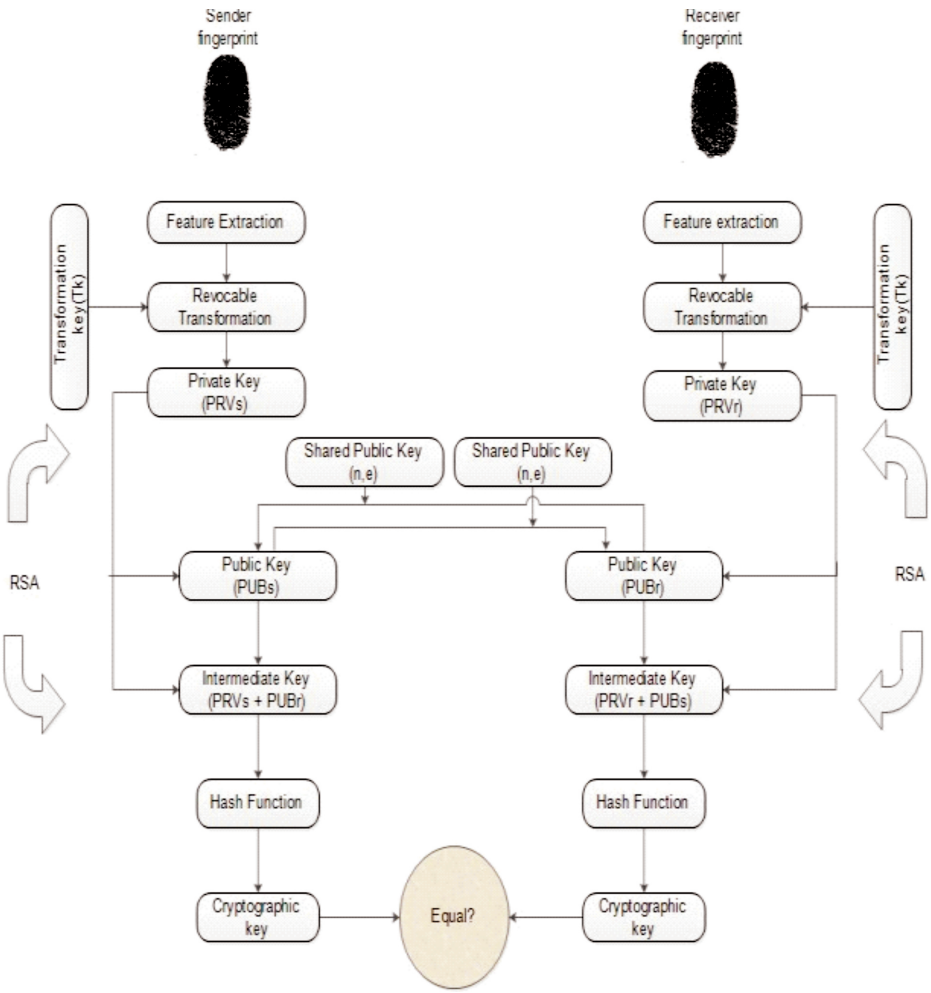

Figure 3. Architectural Design

hashed to generate final cryptographic key. This key is then used for encryption and decryption of information to be shared between sender and receiver.

5.1 Authentication Framework: Salted Hash

In this research work, user authentication is required before communication can be initiated among users. For this, a salted hash algorithm for the password enrolment and verification of users is done. A 'salt' is any random data generated through a salting algorithm that is used as an additional entry or input to a One–Way Password Function. This allows authentication for those who use one password for many system or websites to be secured from attack even if that password is compromised. For this singular reason, salting algorithms are kept private to make cryptanalysis of system password extremely hard. Figure 4 represents the block diagram of the salting hash process.

5.2 Use case diagram

The use case diagram in Figure 5 comprises of three actors: the sending user, the system module, the recipient and displays how they interact with each other.

The sending user needs to be registered first by providing user specific credentials that is used to create the user account in the database. The registration extends to the login function, which allows the user to use a part of the already provided credential to log into the system. The successful login of the user further extends the functionality, which allows the user to compose mails encrypted with user data, check the inbox, and change the password.

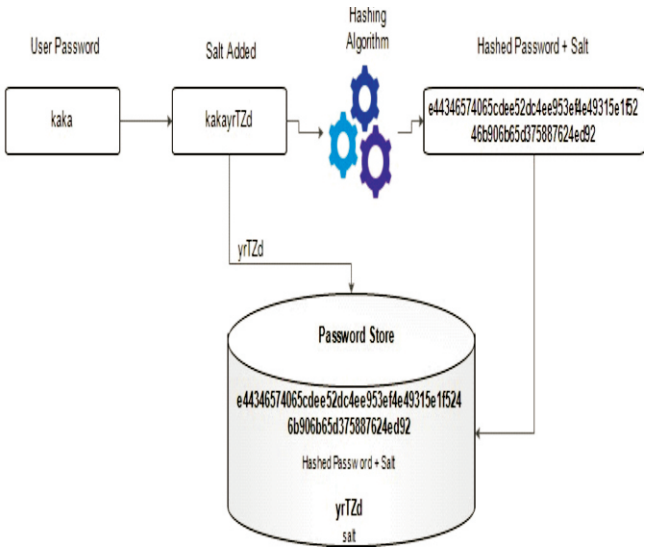

Figure 4. The Salted Hash Process

System Module: This refers to the CryptBio System that runs all the functionalities in the backend or in the background.

Recipient: This user is interchangeable with the sending user as they are dependent on the other if the system is to be used efficiently. Like the sending user, this user must also be registered and have all access rights as the sending user.

6. System Implementation

The detailed implementation of the proposed system is discussed in this section. The core software tools deployed in this system includes Java and MySQL, which is to be deployed for the development of the Graphical User Interface of the system and other coding validation and debugging, while MySQL will be deployed for maintaining the backend database of the system. The choice of Java

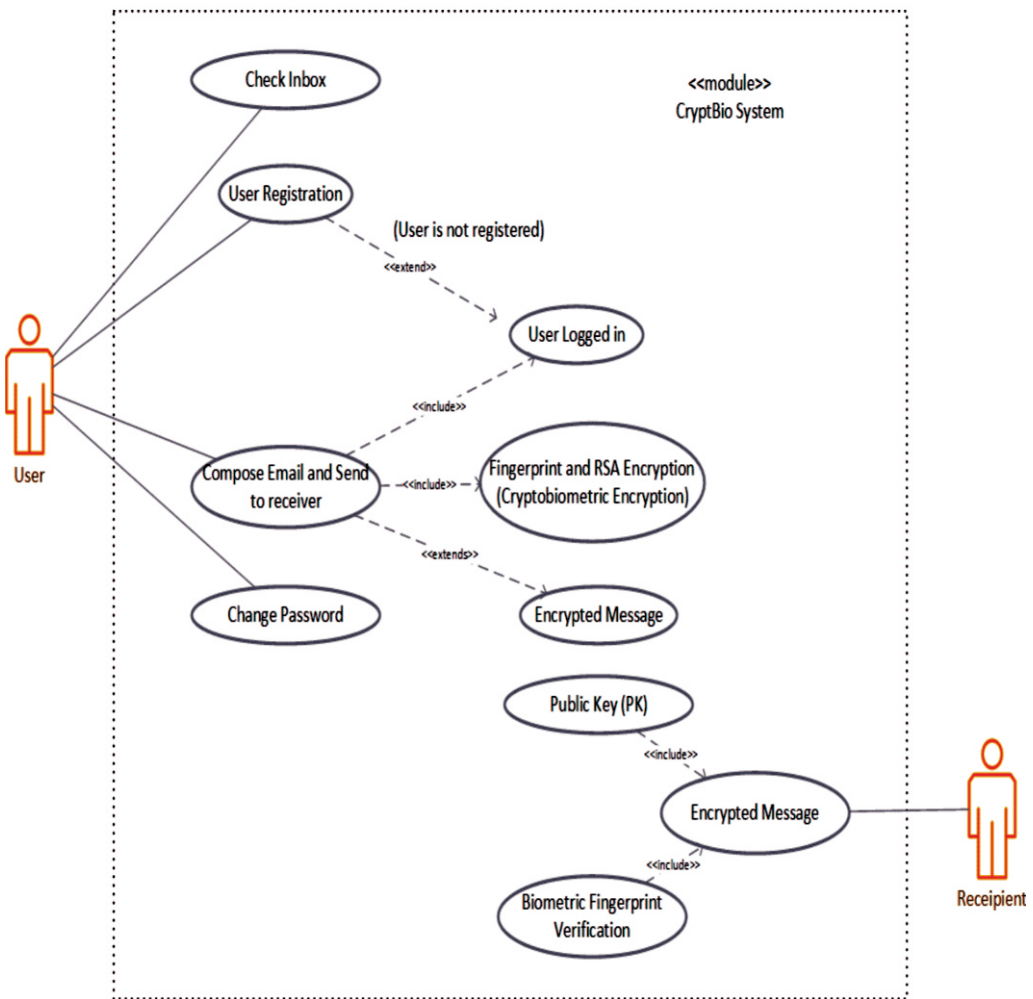

Figure 5. System Use Case Diagram

programming language is designed with security in mind by the developers. It is class-based, object-based and designed to have a implementation dependencies as possible, which can be imported as a library. The database used in the development is MySQL. MySQL is open source, robust and compatible with different operating systems.

6.1 Requirement Analysis of the Proposed System

The requirement specification of this system constitutes the basis for subsequent system design and provides a reference point for any future validation of the developed system. Functional and non-functional requirements are important and are the basic needs to ensure the effective security of data.

6.1.1 Functional Requirements

The core functional requirements of the proposed system include:

- Successful enrolment or registration of users
- Successful authentication and verification of users.
- The ability to encrypt username and password
- The biometric generation of RSA crypto key features captured during registration.
- The system should run a desktop application.

The core non – functional requirements include: User friendly environment, fast processing speed, reliability, ability to flag user-friendly error messages serving as an indication to what problems may have occurred to the user.

6.1.2 Software Requirements

The software requirement for the implementation of the proposed system includes:

- Web application browsers – for database connection
- Java – the used programming language.
- Eclipse 2019 – the Integrated Development Environment used in computer programing for coding, running and debugging the system.
- XAMP server (Windows apache, and MySQL) – provides MySQL database and http apache connection for database management of users data and testing.
- Acceptable operating system (Microsoft windows, Macintosh, Linux, Android, iOS, blackberry)

6.1.3 Hardware Requirements

The following hardware resources are used with the minimum configuration;

A Dell Latitude e5430 Laptop (Specification: 4 GB RAM, Core i5 Intel processor, 2.50 GHz dual core processor speed, 500 GB Hard Drive, and Windows 8 Operating System, 4GB of RAM and DigitalPersona U.are.U biometric software development kit) for fingerprint biometric enrolment and authentication.

7. Implementation and Discussion of Results

The major screenshots of the developed system are shown in this section. GUI startup page is shown in Figure 6.

The general evaluation of the proposed system with the results obtained is carefully discussed in this section. Figure 7 is the first evaluation stage.

From Figure 7, the enrolled user provides his/her credentials, then captures his/her fingerprint image and clicks register. Upon successful registering, the user details are generated in the database, such as username and password which would be used later during login session. After a user provides his authentication credentials, and upon clicking on login, the user details provided would be matched and compared with the database contents. The second step of the user is to compose a message by

Figure 6. GUI Start-up Page

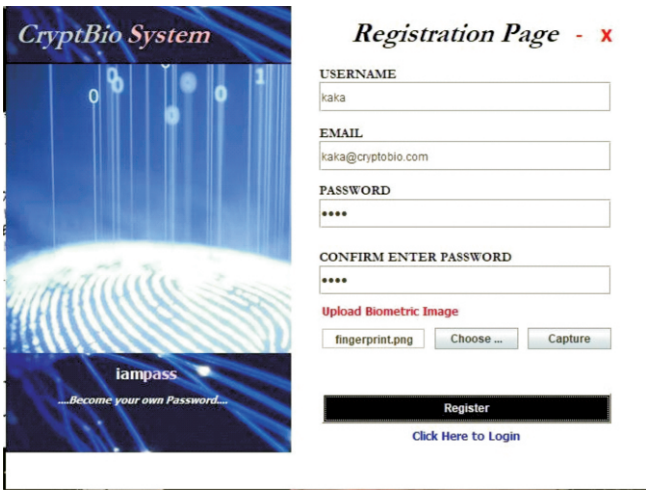

Figure 7. System Evaluation 1

providing the 'To' receiver email address, 'CC' if any, provide the 'Subject' of the message, choose a zip file from memory and click the 'Send' button. The message is sent successfully and encrypted if the 'To' address belongs to an existing system user.

In Figure 8, after clicking on the Inbox, a query fetches the data using the public key 'attached to the user ID' and then loads the table with 'sent received message' from registered system user who has the recipient public key. The same thing happens in the 'Sent' window. The system also provides an avenue for a user to change his/her password.

Figure 8. System Evaluation 2

Conclusion and Recommendation

The purpose of the proposed system is to achieve secure communication. Over the years, fingerprints have served as the most reliable method for personal identification. Enhanced security in communication is achieved by integrating fingerprint biometrics with cryptographic algorithms. The developed system can be deployed as a host-agent application in an intranet.

The architectural framework was designed after the study of some selected independent system models served as the blueprint for the successful implementation of the proposed secure communication system. The implementation of the system was done based on the architectural model suggesting the need for the exploitation of cryptographic algorithms such as RSA and biometric (Fingerprint) integration. The security of the developed system is not limited to communication systems but it is applicable in other security devices. The proposed model is very simple and can be used in desktop systems.

Due to the risen cases of cryptanalysis, information security is critical to the security expert. This study recommends that the fusion of different security techniques cannot be overemphasized to achieve maximum security in an advancing technology that is characterized by daily increase of cyber criminals globally. The main focus of this study was to demonstrate the need for crypto-biometric technique to ensure information security in communication systems. Even though this was achieved, there are uncovered areas which include the extension of this technique to mobile phone devices, the use of error correcting code to normalize the fingerprint data as well as the use of implementation of the techniques using multimodal crypto-biometrics.

References

[1]. Aanjanadevi, S., Palanisamy, V., & Aanjankumar, S. (2019, April). An improved method for generating biometric-cryptographic system from face feature. In 2019, *3rd International Conference on Trends in Electronics and Informatics (ICOEI)* (pp. 1076-1079). IEEE.

https://doi. org/10.1109/ICOEI.2019.8862741

[2]. Adamovic, S., Milosavljevic, M., Veinovic, M., Sarac, M., & Jevremovic, A. (2016). Fuzzy commitment scheme for generation of cryptographic keys based on iris biometrics. *IET Biometrics,* 6(2), 89-96.

[3]. Afriyie, O. K., & Arkorful, V. (2019). Enhancing security of automated teller machines using biometric authentication: A case of a Sub-Saharan University. *Researchgate Publication,* 9(7), 7-22. https://doi.org/10.7176/IKM/9-7-02

[4]. Aggarwal, D., & Maurer, U. (2016). Breaking RSA generically is equivalent to factoring. *IEEE Transactions on Information Theory,* 62(11), 6251-6259. https://doi.org/10.1109/TIT.2016.2594197

[5]. Barman, S., Samanta, D., & Chattopadhyay, S. (2015). Fingerprint-based crypto-biometric system for network security. *EURASIP Journal on Information Security,* 1, 1-17. https://doi.org/10.1186/s13635-015-0020-1

[6]. Chebotareva, A. A., Chebotarev, V. E., & Rozanov, A. S. (2018). Communication society and security: current threats and legal maintenance. In Digital Communication Management. *IntechOpen.* https://doi.org/10.5772/intechopen.75756

[7]. Dwivedi, R., Dey, S., Sharma, M. A., & Goel, A. (2019). A fingerprint based crypto-biometric system for secure communication. *Journal of Ambient Intelligence and Humanized Computing,* 1-15. https://doi.org/10.1007/s12652-019-01437-5

[8]. Jin, Z., Teoh, A. B. J., Goi, B. M., & Tay, Y. H. (2016). Biometric cryptosystems: A new biometric key binding and its implementation for fingerprint minutiae-based representation. *Pattern Recognition,* 56, 50-62. https://doi.org/10.1016/j.patcog.2016.02.024

[9]. Osho, O., Musa, F. A., Misra, S., Uduimoh, A. A., Adewunmi, A., & Ahuja, R. (2019, October). Absolute secure: A tri-layered data security system. In *International Conference on Information and Software Technologies* (pp. 243-255). Springer, Cham. https://doi.org/10.1007/978-3-030-30275-7_19

[10]. Osho, O., Zubair, Y. O., Ojeniyi, J. A., & Osho, L. O. (2014). A simple encryption and decryption system. In Conference: *International Conference on Science, Technology, Education, Arts, Management and Social Sciences (ISTEAMS),* Ado-Ekiti, Nigeria (pp. 77-84).

[11]. Saad, A. M. S. E. (2019, November). A Systematical review study to investigate the use of biometric security techniques in automatic teller machines: Insight from the past 15 years. In 2019, *1st International Informatics and Software Engineering Conference (UBMYK)* (pp. 1-4). IEEE. https://doi.org/10.1109/UBMYK48245.2019.8965494

[12]. Shenoy, K. M., & Shaikh, S. G. (2019, July). An Approach to secure data transmission through the use of cryptography and steganography. In *2019 International Conference on Communication and Electronics Systems (ICCES)* (pp. 1039-1043). IEEE. https://doi.org/10.1109/ICCES45898.2019.9002029

ABOUT THE AUTHORS

Noel Moses Dogonyaro is currently working as a Lecturer in the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria and pursuing Ph.D. degree in Cyber Security Science at the same University. His major area of research includes Post Quantum Computing, Block Chain Technology, Information and Network Security.

Dr. Waziri Onomza Victor is currently working as a Professor of Cyber Security Science. He obtained his Ph.D. in Applied Mathematics at Federal University of Technology, Minna, Nigeria, in 2004. He did his Post Doctorate Fellowship in the Department of Computer Science in 2007, at the University of Zululand, South Africa. He was a Scientific Visiting Fellowship for Africa at the University of Technology, Department of Computer Science /Cryptography Section, Darmstadt, Germany in 2018. His current research field is on Post Quantum Cryptography and Quantum Computing.

Sheidu Kaka Jumai obtained her first degree in Cyber Security Science at Federal University of Technology, Minna, Nigeria. She is currently pursuing her Master of Technology (M.Tech.) degree at the Department of Cyber Security Science, Federal University of Technology, Minna, Nigeria. Her major research areas of interest are Social Engineering, Cyber Self Defence and Network Security.